(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平7－288798

(43)公開日　平成７年(1995)10月31日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｎ　7/16		Ｚ		
Ｇ０９Ｃ　1/00		9364－5Ｌ		
Ｇ１１Ｂ　20/10		Ｈ　7736－5Ｄ		
			Ｈ０４Ｌ　9/ 02	Ｚ
			Ｈ０４Ｎ　5/ 92	Ｈ

審査請求　未請求　請求項の数４　ＦＤ　（全 ９ 頁）　最終頁に続く

(21)出願番号　特願平6－102205

(22)出願日　平成６年(1994)４月15日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　井上　徹
長岡京市馬場図所１番地　三菱電機株式会社映像システム開発研究所内

(72)発明者　倉橋　聡司
長岡京市馬場図所１番地　三菱電機株式会社映像システム開発研究所内

(72)発明者　山田　まさ子
長岡京市馬場図所１番地　三菱電機株式会社映像システム開発研究所内

(74)代理人　弁理士　高田　守

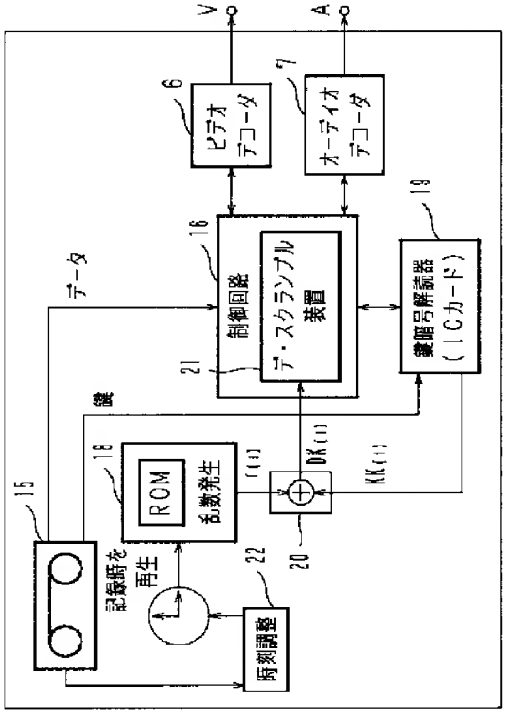
最終頁に続く

(54)【発明の名称】　ディジタル録画記録再生装置及び再生装置並びにＴＶ受信装置

(57)【要約】

【目的】　暗号放送のセキュリティをより高めた方式によるテレビ受像器、また暗号データを暗号されたまま記録し、再生時に暗号をデ・スクランブルして試聴するＶＴＲ装置を得る。

【構成】　データスクランブル用鍵を暗号化し、そのデータを時計情報より更新する乱数と演算し、その得られた鍵を伝送鍵としてパケット形式で伝送を行い、受信側でヘッダー部に暗号がかかっているかどうか判断し、同一時刻の時計より更新される同一の乱数を得てその乱数と、伝送鍵を鍵復号アルゴリズムにより復号するＩＣカード等による鍵暗号解読器によって復元した中間鍵とより演算して求めたデータをデ・スクランブルする鍵を得てデータをデ・スクランブルし、ビデオデータとオーディオデータを復元して試聴するテレビおよび暗号化データをそのまま記録し、所定の演算によって得たデータスクランブル鍵でデータを復元してビデオ、オーディオ信号を再生する。



1

【特許請求の範囲】

【請求項１】　ディジタル信号で放送するプログラム単位にプログラムヘッダーを付けそれを特定のパケットに分割してパケットヘッダーをつけパケットデータをスクランブルして伝送するディジタルＴＶ信号であって、予め決められた鍵暗号化アルゴリズムによりデータのスクランブル鍵を暗号化し中間的な鍵を得て、時計情報によって得られた乱数と演算してデータデスクランブル鍵を暗号化して伝送された信号を受信するものであって、復号側で時計手段よりの情報により乱数を発生させる乱数発生手段、暗号化されて送信されてきたデータスクランブル鍵を解読する鍵暗号解読器、またはＩＣカード手段により解読して得た中間的な鍵と、時計手段により発生させた乱数を演算してデータスクランブル鍵を復号する演算手段を備えてデータを復元することを特徴とするディジタルＴＶ受信装置。

【請求項２】　回転ヘッドを用いて磁気テープにアジマス記録するディジタル録画記録再生装置であって、ＭＰＥＧなどのイントラフレームと予測フレームが混在する伝送方式で、ディジタル信号で送信されてきたプログラムデータをパケット形式で伝送されるビデオ信号を記録再生する録画記録再生装置であって、伝送レートＲｔより記録レートＲｒが大なるレートで記録する装置において、記録する際、伝送パケットのまたはプログラムのヘッダーによってデータが暗号化されているかどうか判断し、あるいはイントラなどのフレームの検出ができないことにより暗号化されていることを判別しデータが暗号化されていない場合はデータを一度復号し、その一部分（例えば特殊再生用のイントラフレームの低域成分）を抽出して伝送されてきたデータ部と受信側で抽出した一部分のデータの両方を記録レートＲｒで記録し、ヘッダー部よりあるいはイントラなどのフレームが検出できないことなどにより暗号化されていると判断される場合はその暗号化されたデータをそのまま記録する記録手段を備えたことを特徴とするディジタル録画記録再生装置。

【請求項３】　請求項２で記録されたテープなどの媒体よりデータを再生する再生装置において特殊再生の時は一部抽出した成分（イントラフレームの低域成分など）により特殊再生時にも連続動画を再生するＶＴＲにおいて、暗号化されたデータを再生するときはテープに記録された復号化鍵を所定の鍵暗号鍵読器やＩＣカードなどにより解読して鍵を再生し、得られた鍵をもとにスクランブルされて記録されたデータをデスクランブルしてデータを再生する再生手段を備えたことを特徴とするディジタル録画再生装置。

【請求項４】　プログラムデータをパケット形式で伝送するデータ伝送信号であって、暗号化されているか否かを示す情報と、データをデ・スクランブルする鍵を暗号化して伝送し復号側で上記信号を受信してデータ鍵を解読する鍵暗号解読器またはＩＣカードによって送信された暗号化鍵を復号して、受信側で時計情報による乱数と、所定の鍵復号アルゴリズムを備えた暗号解読器またはＩＣカードにより伝送された鍵を解読した中間的な鍵とを演算した結果得られたデータスクランブル鍵によりデータを復元することを特徴とするディジタル録画再生装置。

2

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はディジタル映像信号とディジタルオーディオ信号とを受信するＴＶ装置、および、ディジタル映像信号とディジタルオーディオ信号とを、斜めトラックのそれぞれ決められたエリアに記録するようなトラックフォーマットを有するディジタルビデオテープレコーダ（以下、ディジタルＶＴＲという）において、ディジタル映像信号とディジタルオーディオ信号とがビットストリームで入力され、このビットストリームを記録するディジタルＶＴＲに係わり、特にそれらの暗号化されたデータの伝送と記録と再生に関するものである。

【０００２】

【従来の技術】図６は一般的な家庭用ディジタルＶＴＲのトラック図である。図において、磁気テープには斜めトラックが構成されており、一つのトラックはディジタル映像信号を記録する映像エリアと、ディジタルオーディオ信号を記録するオーディオエリアの二つのエリアに分割されている。

【０００３】このような家庭用ディジタルＶＴＲに映像およびオーディオ信号を記録するには二つの方法がある。一つは、アナログ映像信号とオーディオ信号を入力として、映像やオーディオの高能率符号化器を用いて記録する、いわゆるベースバンド記録方式である。もう一つは、ディジタル伝送されたビットストリームを記録する、いわゆるトランスペアレント記録方式である。

【０００４】アメリカ合衆国で審議されているＡＴＶ（Ａｄｖａｎｃｅｄ　Ｔｅｌｅｖｉｓｉｏｎ）信号を記録するには、後者のトランスペアレント記録方式が適している。その理由は、ＡＴＶ信号は既にディジタル圧縮された信号であり、高能率符号化器や復号化器が不要であることや、そのまま記録するので画質の劣化がないことなどである。

【０００５】上述のようなＡＴＶ信号を記録するディジタルＶＴＲの方式として、１９９３年１０月２６日から２８日にカナダ国オタワ市で開催された“Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｗｏｒｋｓｈｏｐ　ｏｎ　ＨＤＴＶ’９３”における技術発表に、“Ａ　Ｒｅｃｏｒｄｉｎｇ　Ｍｅｔｈｏｄ　ｏｆ　ＡＴＶ　ｄａｔａ　ｏｎ　ａＣｏｎｓｕｍｅｒ　Ｄｉｇｉｔａｌ　ＶＣＲ”がある。以下、この内容を従来例として述べる。

【０００６】家庭用ディジタルＶＴＲのプロトタイプの基本仕様として、ＳＤ（Ｓｔａｎｄａｒｄ　Ｄｅｆｉｎ

ｉｔｉｏｎ）モード時、ディジタル映像信号の記録レートを２５Ｍｂｐｓとして、フィールド周波数が６０Ｈｚの場合、映像の１フレームを１０トラックの映像エリアに記録するものがある。ここで、ＡＴＶ信号のデータレートを１７－１８Ｍｂｐｓとすると、このＳＤモードでＡＴＶ信号のトランスペアレント記録が可能になる。

【０００７】図７はディジタルＶＴＲの通常再生時と、高速再生時におけるヘッドトレース図である。図において、各トラックは違ったアジマス角度を持つヘッドにより交互に斜め記録されている。通常再生時は、テープ送り速度が記録時と同じであるので、ヘッドは記録トラックに沿って、図７（ａ）のようにトレースすることができる。しかし、高速再生時はテープ速度が異なるためいくつかのトラックを横切ってトレースし、各同一アジマストラックの断片のみを再生することができる。図７（ｂ）では５倍速の早送りの場合を示す。

【０００８】ＭＰＥＧ２のビットストリームでは、イントラ符号化されたブロックのみが他のフレームを参照せずに独立に復号できる。もし、ＭＰＥＧ２のビットストリームが順番に各トラックに記録されているとしたら、高速再生時の再生データは固まって飛び飛びにバースト状に再生されるので、イントラ符号化されたブロックのみで画像を再構成することになる。このとき、スクリーン上では、再生されるエリアは連続ではなく、また、ブロックの断片がスクリーンに広がることになる。さらに、ビットストリームは可変長符号化されているので、スクリーンのすべてが周期的に更新される保証はなく、ある一部が長い時間更新されないこともある。

【０００９】図８は高速再生が可能なビットストリーム記録装置のブロック図である。ここでは、各トラックの映像エリアを、全てのＡＴＶ信号のビットストリームを記録するメインエリアと、高速再生時に画像の再構成に用いるビットストリームの重要な部分（ＨＰデータ）を記録する複写エリアとに分ける。高速再生時は、イントラ符号化ブロックのみが有効であるので、複写エリアにこれを記録するが、さらにデータを削減するために、すべてのイントラ符号化ブロックから低域周波数成分を抜き出して、ＨＰデータとして記録する。図８において、１０１はビットストリームの入力端子、１０２はビットストリームの出力端子、１０３はＨＰデータの出力端子、１０４は可変長復号器、１０５はカウンタ、１０６はデータ抜き取り回路、１０７はＥＯＢ（Ｅｎｄ　ｏｆ　Ｂｌｏｃｋ）付加回路である。

【００１０】ＭＰＥＧ２のビットストリームは入力端子１０１から入力され、出力端子１０２からそのまま出力されて、メインエリアに順次記録される。一方、入力端子１０１からのビットストリームは可変長復号化器１０４にも入力され、ＭＰＥＧ２のビットストリームのシンタックスが解析され、イントラ画像を検出し、カウンタ１０５にてタイミングを発生し、データ抜き取り回路１０６でイントラ画像のすべてのブロックの低域周波数成分を抜き出し、さらに、ＥＯＢ付加回路１０７でＥＯＢを付加して、ＨＰデータを構成し、複写エリアに記録する。

【００１１】図９は、図８の装置の再生時の動作を示す図である。通常再生時はメインエリアに記録されているすべてのビットストリームが再生され、ディジタルＶＴＲの外にあるＭＰＥＧ２復号器に送られる。ＨＰデータは捨てられる。一方、高速再生時は、複写エリアのＨＰデータのみが集められて復号器に送られ、メインエリアのビットストリームは捨てられる。

【００１２】図１０はテープ上のメインエリアと複写エリアの例を示す図である。家庭用ディジタルＶＴＲでは、各トラックの映像エリアは１３５のシンクブロックから構成されており、メインエリアは９７シンクブロック、複写エリアは３２シンクブロックとした。この場合、メインエリアのデータレートは約１７．４６Ｍｂｐｓ、複写エリアは１７回同じデータが記録されるので、約３３８．８ｋｂｐｓとなる。

【００１３】図５は従来の暗号化放送に用いるテレビ装置とその放送データを録画するＶＴＲの説明図である。ＢＳ（放送衛星）テレビ放送ではコアテック方式が用いられている。（文献１、昭和６２年度電機通信技術審議界答申諮問　第１８号監修）ＢＳの暗号方式はラインローテーションとラインパーミュテーション方式があり、ラインローテーションはテレビ画面の１フレームまたは１フィールドの各走査線内の信号を切り替える方式、ラインパーミュテーションは走査線どうしを適宜入れ換えることによりスクランブルをかける。従来ＢＳまたはＣＳの暗号放送は契約するとき暗号デコード装置を購入しユーザーはそれを受信機に付加する。この時ユーザーのＩＤ番号が登録される。使用者は使用期間の料金を支払いその間は電波によって送られてきた暗号デスクランブル鍵を自動的に解読器が解読してそれによって送信側でスクランブルされたデータをデスクランブルして視聴していた。デコード装置はＴＶ受像器に内蔵されているものもあった。各デコーダは向上出荷時マシーン個別のＩＤ番号がつけられる。またＣＳテレビ放送では５つのスクランブル方式があり各種委託放送事業者はこれらの方式（①コアテック方式、②Ｍ方式、③スカイポート方式、Ｂ－ＮＴＳＣビデオサイファー方式、⑤Ｂ－ＭＡＣ方式）を自由に選択できる（文献２、泉　武博「ケーブルテレビ技術入門一（基礎から応用まで）」コロナ社）には放送にスクランブルを用いる技術が詳述されている。図５でＳＭはスクランブルされたデータを復号するための鍵を解読するための鍵暗号鍵読器または解読アルゴリズムを備えたＩＣカードであり、この装置で送信されてきた鍵を解読してデータをデ・スクランブルする鍵を得て元のデータを復元する。復元されたデータは通常のアナログまたはディジタルのＶＴＲにそのまま接続す

5

れば暗号を復号した状態で通常の番組の録画と同じように録画が可能である。

【００１４】

【発明が解決しようとする課題】しかし、この方式はＴＶ用の暗号スクランブルのデコーダーを購入した人は一度デスクランブルされたＴＶ信号をその出力端子よりＶＴＲにそのまま記録することができ以後無制限にダビングが可能になるという著作権上の課題があった。また、留守番録画を行いＶＴＲで暗号放送を記録して見たいユーザーと録画はしないが、ＴＶは暗号放送も視聴したいユーザーとを分離できないという課題があった。

【００１５】本発明上記のような課題を解決するためになされたもので、暗号放送のセキュリティをより高めた方式によるディジタルＴＶ受信装置、また、暗号データを暗号されたまま記録し、再生時に暗号をデ・スクランブルして試聴するディジタル録画記録再生装置及びディジタル録画再生装置を提供することを目的とする。

【００１６】

【課題を解決するための手段】本発明の請求項１に係るディジタルＴＶ受信装置は、復号側で時計手段よりの情報により送信側に同期して同じ手順で乱数を発生させる乱数発生手段、送信されてきた暗号化されたデータスクランブル鍵を解読する暗号解読器、またはＩＣカード手段により解読して得た中間的な鍵と時計情報により発生させた乱数を演算してデータスクランブル鍵を復号する演算手段を備えてデータを復元するものである。

【００１７】本発明の請求項２に係るディジタル録画記録再生装置は、伝送パケットのまたはプログラムのヘッダーによってデータが暗号化されているかどうか判断する手段、あるいはイントラなどのフレームの検出ができないことにより暗号化されていることを判別する手段、データが暗号化されていない場合はデータを一度復号し、その一部分（例えば特殊再生用のイントラフレームの低域成分）を抽出して伝送されてきたデータ部と受信側で抽出した一部分のデータの両方を記録レートＲｒで記録し、ヘッダー部より暗号化されていると判断される場合はその暗号化されたデータをそのまま記録する記録手段を備えたものである。

【００１８】本発明の請求項３に係るディジタル録画再生装置は、暗号化されたデータを再生するときはテープに記録された復号化鍵を所定の鍵暗号鍵読器やＩＣカードなどにより解読して鍵を再生し、得られた鍵をもとにスクランブルされて記録されたデータをデスクランブルしてデータを再生するデ・スクランブル手段を備えたものである。

【００１９】本発明の請求項４に係るディジタル録画記録再生装置は、時計情報により作成された乱数と、所定の鍵暗号アルゴリズムで暗号化した鍵との演算結果を伝送し、受信側で時計手段よりの情報により乱数を発生する算数発生手段、所定の鍵復号アルゴリズムを備えた暗

6

号解読器またはＩＣカード、により伝送された鍵を解読した中間的な鍵を時計よりの乱数と演算する演算手段、その結果得られたデータスクランブル鍵によりデータを復元するデ・スクランブル手段を備えたものである。

【００２０】

【作用】本発明は送信されてきた暗号化データをＶＴＲに暗号化されたデータのまま記録し正当なユーザーが正当な手続きで記録再生することができる暗号解読デコーダまたはＩＣカードを備えているのでＴＶとＶＴＲを独立の別々の契約で放送を試聴することができＶＴＲの契約者は留守番録画などにより暗号スクランブルデータのまま一旦録画し、後日暗号解読器またはＩＣカードにより暗号化鍵を解読してデータのスクランブル鍵を復号して試聴することが出来る。

【００２１】本発明の請求項１に係るディジタルＴＶ受信装置においては、時計情報より定期的に更新される乱数情報発生し、予め決められた鍵暗号アルゴリズム実行手段とにより演算をする演算手段を備えてデータをスクランブル、デ・スクランブルする鍵を暗号化する作用がある。

【００２２】本発明の請求項２に係るディジタル録画記録再生装置においては、ヘッダー情報によって暗号化されているかどうかを判別し暗号化されていないときはデータを復号し、その一部を抽出して記録レートＲｒで記録しヘッダー情報により暗号化されていないと判断した場合はそのデータを暗号化されたままで記録する作用がある。

【００２３】本発明の請求項３に係るデイジタル録画再生装置においては、暗号化されたデータを再生するときテープに記録された伝送鍵をＩＣカードなどの鍵暗号鍵読手段により解読してデータのデ・スクランブル鍵を取り出す作用があり、暗号化されて記録されたデータからデータをデ・スクランブルして元のビデオ、オーディオデータを復元する作用がある。

【００２４】本発明の請求項４に係るディジタル録画再生装置においては、記録された時刻情報より再生した記録時の時計情報を得る作用あるいは記録された時刻情報より調整して記録時の時刻情報を再生する作用があり、ＩＣカードなどの鍵暗号解読手段と併せ用いて演算する作用がある。

【００２５】

【実施例】

実施例１．図１は本発明に係るてＴＶ受信装置を示すブロック図である。図において、１はディジタルテレビ信号入力端子、２はモデムおよびヘッダーデコード手段、３は時計機能手段、４は乱数発生手段、５は制御回路によるコントロール手段、６はビデオ信号デコード手段、７はオーディオ信号デコード手段、８は鍵暗号解読器、またはＩＣカード、９は演算手段Ｉ、１０はスクランブル手段、１１はビデオ信号出力端子、１２はオーディオ

信号出力端子である。

【００２６】図２は伝送されたデータからデ・スクランブルする鍵を復号するシーケンスを説明する図である。端子１より入力された受信ディジタルＴＶ信号は２のモデム手段によりディジタルパターンに復調される。データは放送プログラム毎にプログラムヘッダーが付加された後、パケット単位に分割される。各パケットはパケットヘッダーが先頭に付加される。こうして伝送されたベースバンドのディジタル信号が再生され、プログラムヘッダーおよびパケットヘッダーの解読が行われる。図で制御回路５は受信データよりデータ鍵を運搬する送信鍵ＴＫ（ｉ）を受信データより抽出して暗号解読器８へ送り、中間的な鍵出力ＫＫ（ｉ）を得る。ＫＫ（ｉ）は演算装置Ｉ ９へ入力される。一方、時計情報より発生された乱数ｒ（ｉ）が演算装置Ｉ ９へ入力され演算結果としてＤＫ（ｉ）を得る。時計情報より発生された乱数ｒ（ｉ）とはスクランブル、デ・スクランブルに用いられる乱数は例えば同一ＰＮ（ｐｓｅｕｄｏ　ｎｏｉｓｅ）シーケンスを発生するシフトレジスターを送信、受信でデータに法２加算して送信し、受信側で送信データに対応させて同一のＰＮシーケンスパターンを法２加算して元の情報を得る。この場合、スクランブルの初期値が鍵となる。このＤＫ（ｉ）がデータを直接スクランブルした時の鍵に対応する復号鍵であるのでデ・スクランブル装置１０へ送ってデータを復元し、ビデオ部分はビデオデコーダ６へ、オーディオ部分はオーディオデコーダ７へ送り、各々デコードしてビデオ出力およびオーディオ出力を得る。

【００２７】パケットヘッダーには各パケットが暗号化されているかどうかを示すフラグがかかれており、プログラムのヘッダーはパケットの後に続いてかかれ、暗号化されたデータの場合は特定のいくつかのフィールドに繰り返してデ・スクランブルするための鍵情報がかかれる。

【００２８】図２ではプログラムパケットが大きいときはプログラムを適当なパケットづつ区切って伝送パケットとプログラムパケットの中間的な適当な大きさの、いわばスクランブルユニット単位のストリームにし、その単位で鍵を配送する。プログラムパケットが小さいときは鍵の更新は以下のようにする。図２で一番上のシーケンスは送信鍵が送られてくる状態を示したもので各伝送パケットのヘッダーに奇数番目か偶数番目かの区別を示すフラグがあり、それに基づいて常に２つの鍵が送られてくる。その様子がいちばん上の送信鍵シーケンスである。図の点線は時刻ｉの鍵データはＴＫ（ｉ）を受信してから時間ＴＡ の間にデータ鍵を解読してＤＫ（ｉ）なる鍵を得る。一方、時計情報からの乱数ｒ（ｉ）を得て、それを所定の演算（例えば、いちばん簡単な例では法加算）を行い、ＤＫ（ｉ）を例えば、

ＤＫ（i）＝ｒ（ｉ）＋ＫＫ（ｉ）

より得る。但し、ここで＋記号は法２加算を示し、ＥＸＯＲ（Exclusiv OR;排他的論理和）で実現される。得られた鍵ＤＫ（ｉ）は送信側でデータをスクランブルした鍵に同じになるので、これを例えば、データに法２加算してデータを取り出す。

Ｉ（ｉ）＝ＤＡＴＡ（ｉ）＋ＤＫ（ｉ）

ここで、ＤＡＴＡ（ｉ）は送られてきたプログラムデータである。このようにしてビデオとオーディオのディジタル情報を復元したのちビデオ信号はビデオデコーダ６でオーディオ信号はオーディオデコーダ７で各々復号して各々ビデオ出力、オーディオ出力を端子Ｖ、Ａより出力する。

【００２９】ここで、時計情報による乱数とは図２の送信鍵シーケンスＴＫ（ｉ）より得られた中間的な復号鍵系列ＫＫ（ｉ）と同じ更新時間間隔で乱数ｒ（ｉ）を発生するもので送信、受信で例えば同一のＲＯＭにかかれた乱数データを正確な時計を送信、受信で同期させて中間的な復号鍵系列ＫＫ（ｉ）と同じ更新時間期間で乱数を発生させる。正確な時計情報で同一ＲＯＭなどに記録されている乱数データを更新して乱数を発生する。演算装置９は送信、受信で同じ演算アルゴリズムを持ち発生させた乱数ｒ（ｉ）を復号鍵ＫＫ（ｉ）を入力して一定の演算を行い、データ復元用デ・スクランブル鍵ＤＫ（ｉ）を得る。

ＤＫ（ｉ）＝Ｆ（ＫＫ（ｉ），ｒ（ｉ）；ｉ）

で与えられる。Ｆ（・）はＫＫ（ｉ）とｒ（ｉ）の関数となる。このようにしてデータ復元鍵ＤＫ（ｉ）を得てスクランブル手段１０でデータを復元しビデオ信号はビデオデコーダ、オーディオ信号はオーディオデコーダで元のビデオ信号、オーディオ信号を得て各々端子Ａ，Ｖより出力する。

【００３０】実施例２．図３は本発明によるＶＴＲの記録時の動作を説明する図であり、図４は本発明によるＶＴＲの再生時の動作を説明する図である。図において、１３はディジタルＴＶ信号入力端子、１４はモデムおよびヘッダーデコーダー、１５は記録を行うカセットテープ、１６は制御回路、１７は記録時刻を示す時計機能である。

【００３１】図４で１８は時計情報より乱数を発生させる乱数発生手段、１９はＩＣカードなどによる鍵暗号解読手段、２０は復号鍵ＤＫ（ｉ）を演算して出力する演算手段II、２１はデータを復元するためのデ・スクランブル手段、２２はカセットテープよりの再生時刻情報より送信時刻を再現してそれにより時計機能を入力させて送信時の欄数を発生させる時刻調整機能である。

【００３２】まず、記録動作について説明する。端子１３より入力されたディジタルＴＶ信号は１４のモデムでベースバンド信号になりヘッダーデコーダーで暗号化されているかどうかなどの制御情報や時刻、番組情報、契約や課金情報、個別（ペイパービューか、契約種別、フ

ラットフィー情報など）情報などを取り出す。プログラムまたは伝送パケットのヘッダーによってデータが暗号化されているかどうか判別出来ない時はイントラなどのフレーム検出ができないことにより暗号化されていると判断する。この時、暗号化データをそのままカセットに記録すると同時に記録時の時刻情報をカセットに同時に記録しておく。個別情報には全有料番組が視聴できるフラットフィー（Ｆｌａｔ－ｆｅｅ）契約、例えば映画番組、スポーツ番組のみが試聴できるティア（Ｔｉｅｒ）契約、試聴した分だけ料金を支払うペイパービュー（Ｐａｙ－ｐｅｒ－Ｖｉｅｗ）がある。ヘッダー部にはプログラムの開始時刻や終了時刻など各種時刻情報が入っているのでそれらを記録する。カセットテープに番組の録画と同時に記録する、又書いてない場合は１７のＶＴＲが内蔵している正確な時計により記録時の時刻情報をカッセットに記録しておく。

【００３３】再生時には暗号化データが制御回路のなかのスクランブル手段へ入力されてデータが復元される。ここで用いられるデータ復元鍵ＤＫ（ｉ）の再生について述べる。送信時の鍵ＴＫ（ｉ）は送信時の鍵暗号アルゴリズムに対応した鍵解読アルゴリズムを内蔵したＩＣカードなどの鍵暗号鍵読手段によって中間的な解読鍵ＫＫ（ｉ）　が得られる。一方、カセットテープより記録時の時刻情報が再現されその情報をもとにＶＴＲの時計機能を記録時の時刻に同期させる。乱数発生手段１８は再生された記録時の時計により得られた時刻情報より送信時のスクランブルデータに対応した乱数ｒ（ｉ）を発生し演算手段II２０へ送る。演算手段II２０では入力されたｒ（ｉ）とＫＫ（ｉ）より所定の演算を行いデータをデ・スクランブルする鍵ＤＫ（ｉ）を得る。

【００３４】このようにして、データ用のデ・スクランブル鍵が復号できたのでデ・スクランブル手段によってデータを復元し、ビデオデコーダ６、オーディオデコーダ７で元のビデオ、オーディオ信号を得る。なお、以上は鍵暗号化鍵、鍵復号化鍵が同じ鍵を用いる慣用暗号系を用いる例で説明したが鍵暗号化鍵と鍵復号化鍵が異なる公開鍵を用いる方式でも同一の効果がえられることはあきらかである。

【００３５】公開鍵暗号系は暗号化鍵ｒと復号化鍵ｓが異なっており復号化鍵は秘密に保持されるが暗号化鍵ｒは公開されている。代表的な公開鍵暗号であるＲＳＡ暗号の場合、平文ａに対して暗号文ｂを、

$$b = a^r \pmod{n}$$

より計算して求める。ｎは大きな２つの素数ｐ，ｑの積で与えられる。解読側ではこれをｓ乗する。

$$b^s = a^{rs} = a \pmod{p} = a \pmod{q}$$

であるので、

$$\therefore b^s = a \pmod{n}$$

となり平文ａが復元される。ＲＳＡ暗号はこのように法ｎの演算で実行される。従って公開鍵暗号を用いても暗号化鍵を公開するしないは本発明の基本的な部分でないのでデータスクランブル鍵ＤＫ（ｉ）を暗号化する鍵ｒ。（ｉ）で行い、ＩＣカード等による鍵解読器による鍵復号演算をＲＳＡ暗号の復号化技ｓ。（ｉ）を用いれば慣用暗号とあとは同様に扱えばよい。

【００３６】

【発明の効果】本発明は送信されてきた暗号化データをＶＴＲに暗号化されたデータのまま記録し正当なユーザーが正当な手続きで記録再生することができる鍵暗号解読デコーダまたはＩＣカードを備えているのでＴＶとＶＴＲを独立の別々の契約で放送を試聴することができＶＴＲの契約者は留守番録画などにより暗号スクランブルデータのまま一旦録画し、後日鍵暗号解読器またはＩＣカードにより暗号化鍵を解読してデータのスクランブル鍵を復号して試聴することが出来る。

【００３７】本発明の請求項１に係るディジタルＴＶ受信装置によれば、時計情報より定期的に更新される乱数情報発生手段と、予め決められた鍵暗号アルゴリズム実行手段とにより演算をする演算手段を備えてデータをスクランブル、デ・スクランブルする鍵を暗号化しているのでよりセキュリティ効果の高いテレビ受像器が実現できる効果がある。

【００３８】本発明の請求項２に係るディジタル録画記録再生装置によれば、ヘッダー情報によって暗号化されているかどうかを判別し暗号化されていないときはデータを復号し、その一部を抽出して記録レートＲｒで記録し、ヘッダー情報により暗号化されていないと判断した場合はそのデータを暗号化されたままで記録する記録手段を備えているので、暗号化されたデータでもＶＴＲに記録再生する効果がある。

【００３９】本発明の請求項３に係るディジタル録画再生装置によれば、暗号化されたデータを再生するときテープに記録された伝送鍵をＩＣカードなどの鍵暗号鍵読手段により解読してデータのデ・スクランブル鍵を取り出す機能を有しているので暗号化されて記録されたデータから再生されたデータをデ・スクランブルして元のビデオ、オーディオデータを復元できる効果がある。

【００４０】本発明の請求項４に係るディジタル録画再生装置によれば、記録された時刻情報より再生した記録時の時計情報を得る手段あるいは記録された時刻情報より調整して記録時の時刻情報を再生する手段を備えているのでＩＣカードなどの鍵暗号解読手段と併せ用いて演算することによりデ・スクランブル鍵を得ることができそれによって記録された暗号化データをデ・スクランブルしてビデオ、オーディオ信号を復元する効果がある。

【図面の簡単な説明】

【図１】　本発明に係るＴＶ受信装置を示すブロック図である。

【図２】　伝送されたデータからデ・スクランブルの鍵を復号するシーケンスを説明する図である。

11

【図３】　本発明のＶＴＲの記録時の動作を説明する図である。

【図４】　本発明のＶＴＲの再生時の動作を説明する図である。

【図５】　従来のスクランブル放送を受信するテレビとＶＴＲの説明図である。

【図６】　一般的な家庭用ディジタルＶＴＲのトラック図である。

【図７】　ディジタルＶＴＲの通常再生時と高速再生時におけるヘッドトレース図である。

【図８】　高速再生が可能なビットストリーム記録装置を示すブロック図である。

【図９】　図８の装置の再生時の動作を示す図である。

12

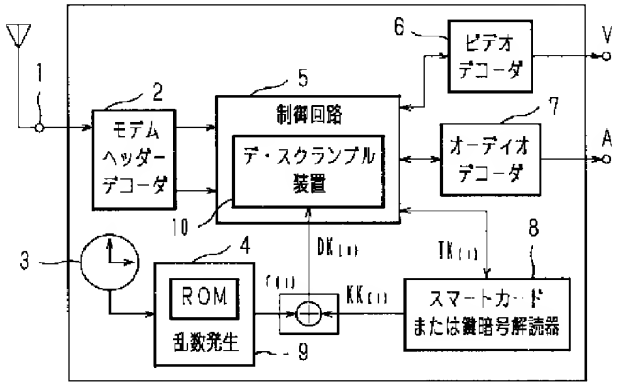
【図１０】　テープ上のメインエリアと複写エリアの例を示す図である。

【符号の説明】

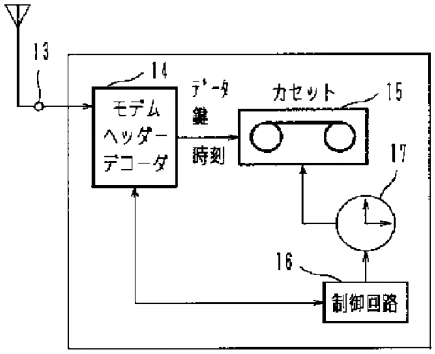
２　ビデオおよびヘッダーデコーダー、３　時計あるいは時刻再生手段、４乱数発生手段、５　制御回路、６　ビデオデコーダー、７　オーディオデコーダー、８　ＩＣカードまたは手段、９　演算手段Ｉ、１０　デ・スクランブル手段、１４　ＶＴＲ内のモデムおよびヘッダーデコーダー、１５　ディジタルＶＴＲカセット、１６　制御回路、１７　時計あるいは時刻再生機能手段、１８　乱数発生器、１９　暗号解読手段、２０　演算手段ＩＩ、２１　デ・スクランブラー

２２　時刻調整手段。

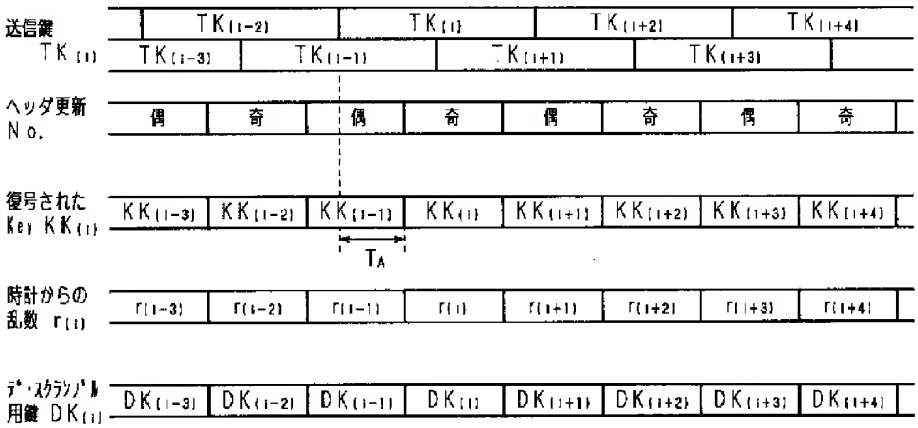
【図１】



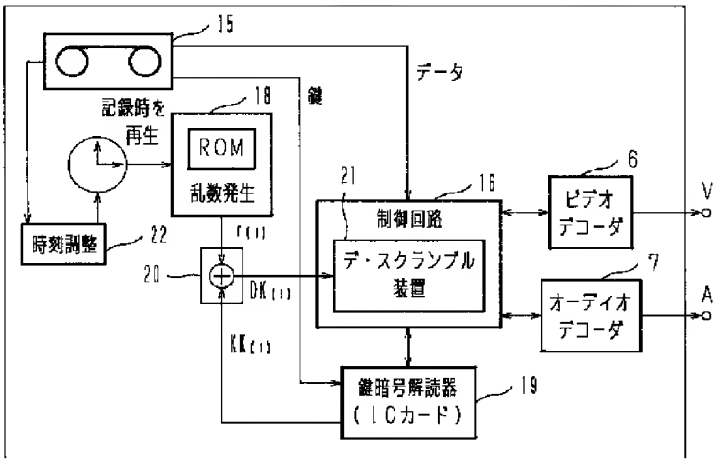
【図３】



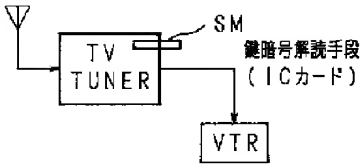
【図２】



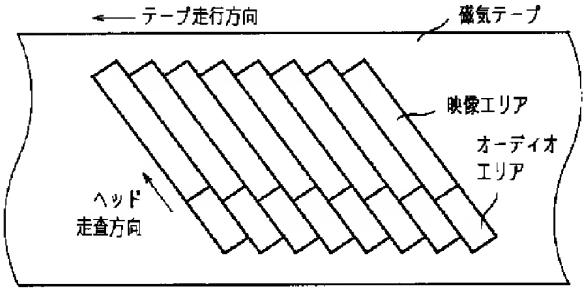
【図４】



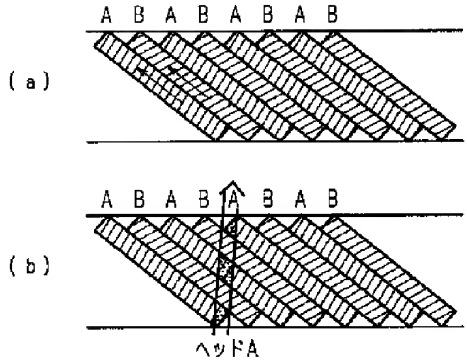
【図５】



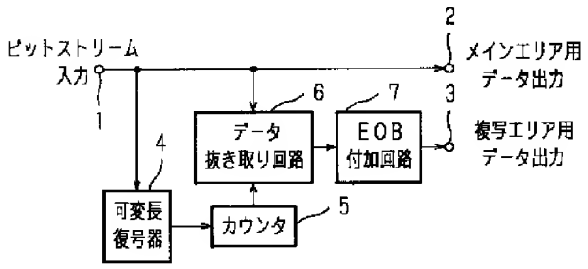
【図６】



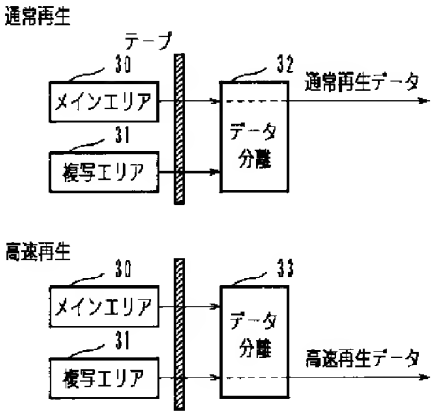
【図７】



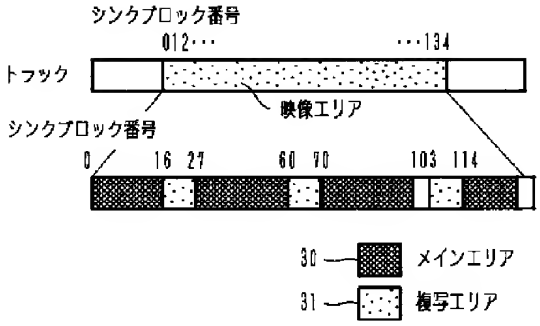
【図８】



【図９】



【図１０】



フロントページの続き

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｋ	1/00		Ｚ			
Ｈ０４Ｌ	9/06					
	9/14					
Ｈ０４Ｎ	5/92					
	7/24					
				Ｈ０４Ｎ	7/13	Ｚ

(72)発明者　山崎　辰男
長岡京市馬場図所１番地　三菱電機株式会
社映像システム開発研究所内